

Free-space quantum key distribution with a high generation rate potassium titanyl phosphate waveguide photon-pair source

Jeffrey D. Wilson^{*a}, Dalton W. Chaffee^a, Nathaniel C. Wilson^a, John D. Lekki^a, Roger P. Tokars^a, John J. Pouch^a, Tony D. Roberts^b, Philip Battle^b, Bertram M. Floyd^c, Alexander J. Lind^a, John D. Cavin^a, and Spencer R. Helmick^a

^aNASA Glenn Research Center, 21000 Brookpark Rd., Cleveland, OH, USA 44135;

^bAdvR, Inc., 2310 University Way, Bldg #1-1, Bozeman, MT, USA 59715;

^cSierra Lobo, Inc., 102 Pinnacle Dr., Fremont, OH, USA 43420

ABSTRACT

A high generation rate photon-pair source using a dual element periodically-poled potassium titanyl phosphate (PP KTP) waveguide is described. The fully integrated photon-pair source consists of a 1064-nm pump diode laser, fiber-coupled to a dual element waveguide within which a pair of 1064-nm photons are up-converted to a single 532-nm photon in the first stage. In the second stage, the 532-nm photon is down-converted to an entangled photon-pair at 800 nm and 1600 nm which are fiber-coupled at the waveguide output. The photon-pair source features a high pair generation rate, a compact power-efficient package, and continuous wave (CW) or pulsed operation. This is a significant step towards the long term goal of developing sources for high-rate Quantum Key Distribution (QKD) to enable Earth-space secure communications. Characterization and test results are presented. Details and preliminary results of a laboratory free-space QKD experiment with the B92 protocol are also presented.

Keywords: photon-pair source, entangled photons, quantum key distribution, quantum communications, B92

1. INTRODUCTION

National Aeronautics and Space Administration (NASA) awarded Small Business Innovative Research (SBIR) contracts in the subtopic Transformational Communications Technology to AdvR, Inc for 'High fidelity down-conversion source for secure communications using on-demand single photons'. Phases I, II, and III were completed in 2010, 2014, and 2015, respectively. The primary goal was to develop a source of entangled photons that could be used to explore both single-photon and entangled-photon quantum key distribution protocols that could eventually enable secure Earth-space communications.

The final product, a high generation rate photon-pair source using a dual element periodically-poled potassium titanyl phosphate (PP KTP) waveguide, was delivered to NASA Glenn Research Center in June of 2015. This paper describes the source, its characterization, and its performance in a preliminary quantum key distribution experiment.

2. PHOTON-PAIR SOURCE

AdvR designed and built the photon-pair source as part of a NASA Phase III SBIR effort. The system integrates a 1064-nm diode laser with a dual element frequency conversion device for generation of photon pairs at 800 nm and 1600 nm. A picture of the non-degenerate photon-pair source is shown in Figure 1.

The photon-pair source integrates a continuous wave (CW) 1064-nm diode laser with a dual element frequency conversion device in which the 1064-nm photons are up-converted to 532 nm in the first section of the waveguide, then down-converted in the second section of the waveguide, where each 532-nm photon has an approximately one in one billion chance of converting into a pair of photons at 800 nm and 1600 nm. The waveguide was similar in design to a dual-element PP KTP waveguide designed for pair generation at 895 and 1310 nm¹.

*Jeffrey.D.Wilson@nasa.gov; phone 1 216 433-3513; fax 1 216 433-8705



Figure 1. The AdvR photon-pair source.

A CW IPS (Innovative Photonics Solutions) diode laser (top) is driven using an ILX Lightwave current source and ILX Lightwave temperature controller. The diode laser is fiber-coupled to an AdvR dual element frequency conversion module (center). The device uses a potassium titanyl phosphate (KTP) waveguide with a periodically-poled grating to frequency double the 1064-nm light to 532 nm. The second grating on the chip is periodically-poled to convert the 532-nm photons into correlated photon pairs at 800 and 1600 nm. The dual element PP KTP module is controlled using a second ILX Lightwave temperature controller. The initial section of the PP KTP waveguide inside the module is a periodically-poled second harmonic generation (SHG) grating to efficiently frequency double the 1064-nm photons to 532 nm, with a poling period of 8.091 μm . The second part of the chip is poled with a period of 8.818 μm for down conversion of the 532 photons to non-degenerate photon pairs at 800 nm and 1600 nm. The input of the waveguide device is coupled with PM980 fiber for efficient transmission from the Innovative Photonics Solutions laser diode. Each section covers half of the 2.11 mm chip length. The output of the device was coupled with PM1550 fiber to mitigate any losses of 1600-nm photons coupling into a single mode fiber which could not support that wavelength. Thus the 800-nm photons, along with any unconverted 1064-nm and 532-nm photons couple into this fiber in a slightly multi-mode manner. The device has an integrated thermal electric cooler with a 10 k Ω thermistor to control the chip temperature. Two temperature controllers from ILX Lightwave control both the diode laser temperature (set at 19°C) and the PP KTP chip temperature (set at 38.7°C).

In the PP KTP waveguide module, at the input fiber-to-waveguide interface, 51% of the 1064-nm light is coupled into the waveguide. The first stage of the waveguide up-converts the 1064-nm light with a conversion efficiency of $\eta = 70\%/W$. If P_{IR} is the amount of 1064-nm light in the waveguide, the amount of 532-nm light generated, P_{SHG} , is $P_{SHG} = \eta P_{IR}^2$. At a laser current of 750 mA, P_{IR} is 115 mW, and there is approximately 9.2 mW of green light generated in the waveguide, and 1.85 mW of green light in the output fiber. The amount of green light generated also depends on the set

temperature of the PP KTP waveguide module. Peak SHG is at a temperature of 38 to 39°C, and at higher powers the temperature depends slightly on the laser drive current.

The CW pump light is delivered to the dual-element module via the input fiber. The output of the fiber is sent to the collection optics breadboard for photon isolation and separation (Figure 2). The photons from the output fiber are collimated by an uncoated asphere and incident on a dichroic mirror. The 800-nm photons (along with most of the 532-nm and 1064-nm light) is reflected into the upper arm in which were placed two dielectric bandpass filters (>97% transmission at 800 nm) to remove the pump and SHG light. The light is then coupled into a multi-mode fiber which delivers the 800-nm photons to a Si single-photon detector. The 1600-nm photons continue through the dichroic mirror and pass through two 1500-nm long-pass filters to remove any residual pump light. A detector is also placed near the open port of the box containing the dichroic mirror. Light rejected from the dielectric filters is scattered out of this open port, and after wavelength filtering, this light can be sent to a detector to monitor the relative quantity of green light being produced by the module. The monitor port can also be used to optimize the module temperature. The 1600-nm photons are also coupled into a multi-mode fiber which delivers the photons to an InGaAs avalanche photodiode (APD).

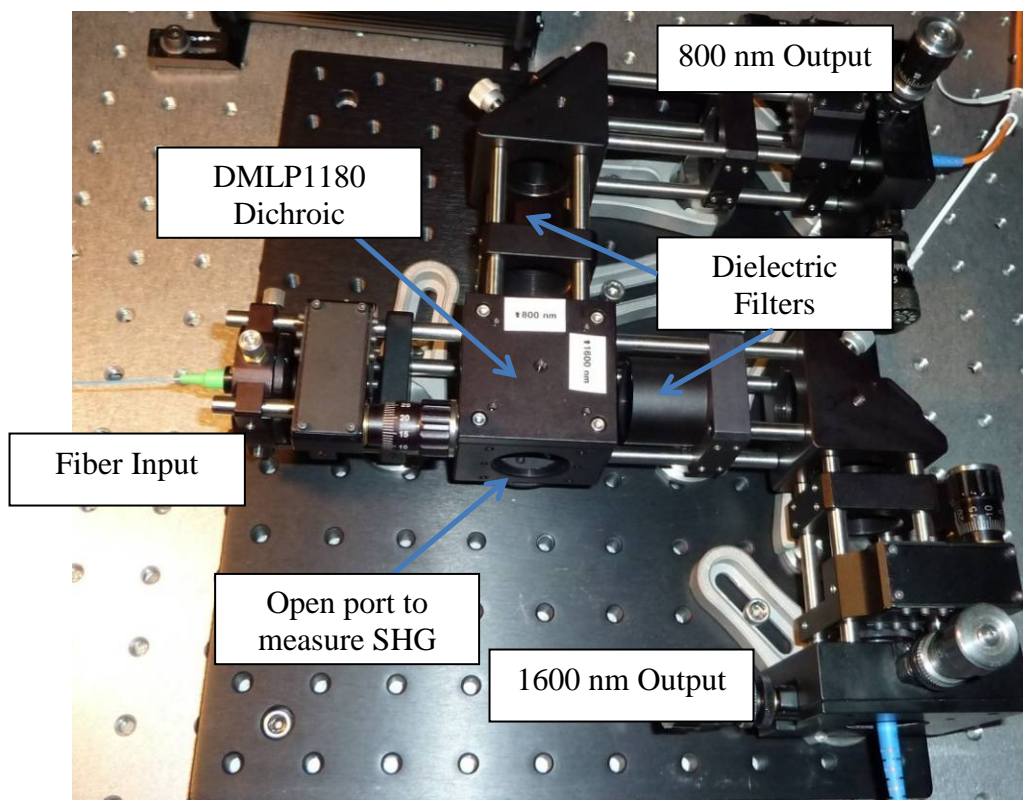


Figure 2. The optical breadboard used to isolate and separate photon pairs from the output fiber of the AdvR photon-pair source.

The theoretical rate of photon pairs produced can be estimated from the following formula:

$$P_S = \eta P_{pump} P_I \quad (1)$$

where P_S is the estimated power of down-converted light generated at the signal wavelength, P_{pump} is the power at 532 nm in this experiment, η is the conversion efficiency of the interaction for the periodically-poled waveguide, and P_I is the idler power. For spontaneous parametric down-conversion, the idler power can be thought of, with hand waving, as the vacuum field at the idler wavelength producing on average one photon (with energy hf) at a rate Δf , where Δf is the frequency bandwidth of the phase-matching interaction^{2,3}, or

$$P_l = hf \Delta f = \frac{hc^2 \Delta \lambda}{\lambda^3} \quad (2)$$

where $\Delta \lambda$ is the phase-matching bandwidth in wavelength instead of frequency. Based on measurements of the photon-pair coincidence rate at AdvR, the inferred photon-pair production rate in the waveguide was 0.74 GHz at $P_{\text{pump}} = 1$ mW. At a predicted down-conversion bandwidth of 4 nm at the 1600-nm wavelength (or 1 nm at the 800-nm wavelength), the conversion efficiency using Equations 1 and 2 can be determined to be $\eta = 160\%/W$, which is a reasonable estimate for expected conversion efficiency of a 1 cm length down-conversion section in a PP KTP waveguide.

3. COINCIDENCE COUNTING

3.1 Experimental Design

We obtain our entangled pairs of 800-nm and 1600-nm photons from the PP KTP source described in the previous section. After the 800-nm and 1600-nm photons are separated by the sorting optics assembly, the 1600-nm photons travel via fiber to an ID Quantique ID210 indium gallium arsenide (InGaAs) detector with the dead time set to its minimum of 1.0 μ s. The output of the ID210 goes through a Stanford Research Systems DG535 delay generator and then into an ID Quantique ID800 coincidence counter. The 800-nm photons are collimated and travel through free space to a PerkinElmer SPCM-AQR-13 silicon avalanche photodiode module⁴. The output of the 800-nm detector runs through a Quantum Composers 9520 delay generator and then into the ID800 coincidence counter. The coincidence counter tags each 800- and 1600-nm count and determines if they occur within 243 ps of each other, which corresponds to a 486 ps coincidence window. We use National Instruments LabVIEW to control the instrumentation and to collect data. We sweep through delay settings on the 800-nm delay generator while recording coincidences. This is repeated for various pump currents. Because the experiment is light-sensitive we turn off all lights and computer monitors and keep the door closed while the experiment runs.

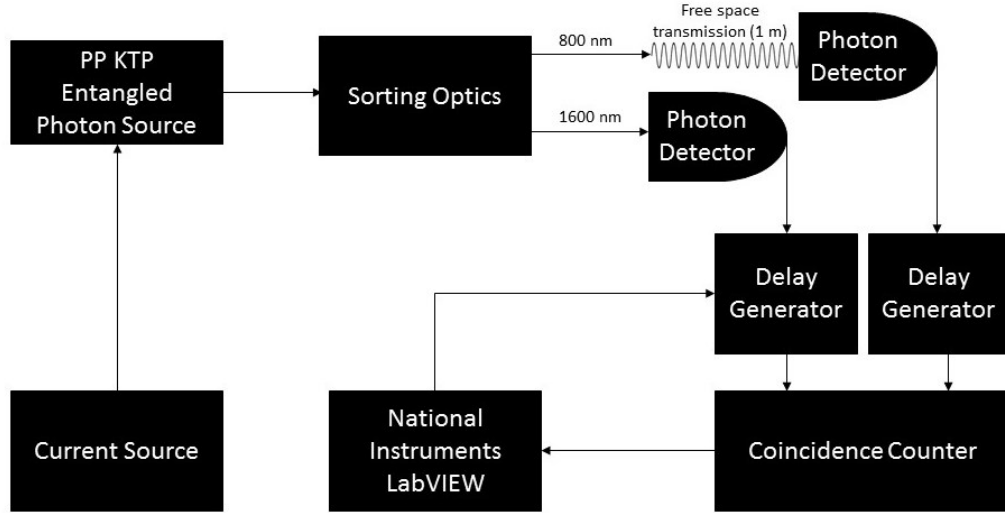


Figure 3. Experimental design.

3.2 Dark Count Study

We performed a dark count study over about an hour under the same lighting conditions as our subsequent studies. All lights and computer monitors were turned off.

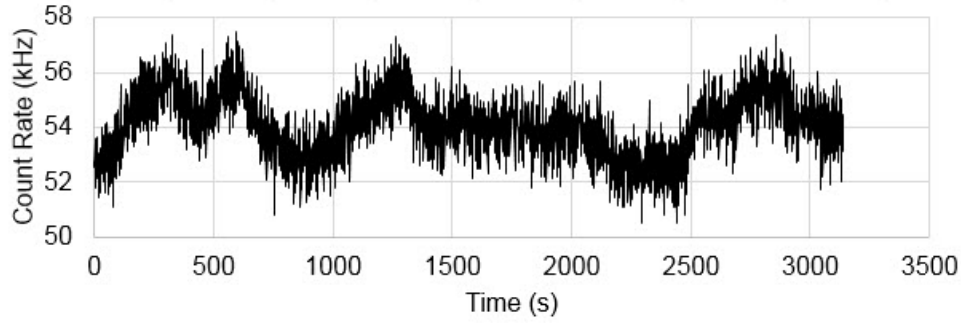


Figure 4. Dark count rate of 800-nm photons versus time. The detector dead time is 50 ns⁴. The average dark count rate was 1.12 kHz.

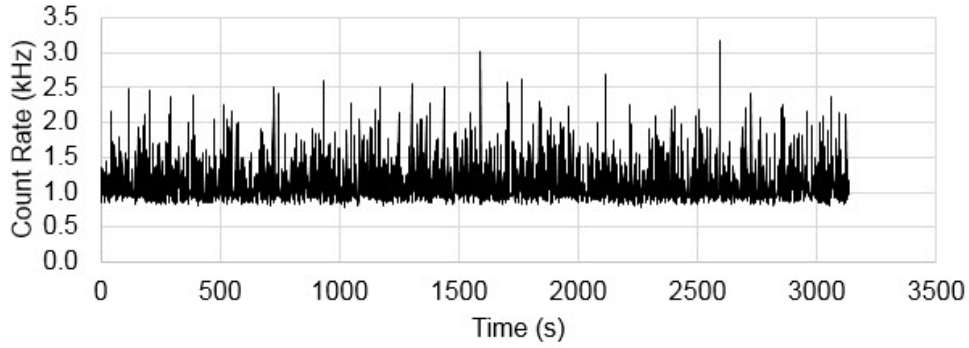


Figure 5. Dark count rate of 1600-nm photons versus time with the detector dead time set to 1 μ s. The average dark count rate was 54.1 kHz.

The average dark count rates obtained were 1.12 kHz for our Si 800-nm detector and 54.1 kHz for the InGaAs 1600-nm detector. These averages were subtracted from future measurements where appropriate. The fluctuations in the 1600-nm detector dark count study are believed to be a characteristic of the detector's cooling cycle.

3.3 Coincidence Results

In order to characterize the source and our detection system, we counted coincident photon detections over a range of delay times. A coincident photon detection in our system is defined by the detection of both an 800-nm and 1600-nm photon within a 486-ps coincidence window. We performed this measurement over a series of delay times in increments of 240 ps around the coincidence peak, averaging coincidence counts over 150 seconds at each delay time to compensate for statistical fluctuations. The 240-ps increment was determined as appropriate resolution given the feature sizes of our coincidence curves, while the 486-ps coincidence window was a multiple of the predetermined bin-width of the coincidence counter. Because our coincidence window was not equal to the delay time increment, we scale each coincidence measurement by a factor of 240/486 to compensate for double or triple counting coincidences at a given delay time (Figure 6). Results were normalized with respect to the number of 800-nm counts to eliminate the effects of small variations in laser power over time scales longer than the integration time.

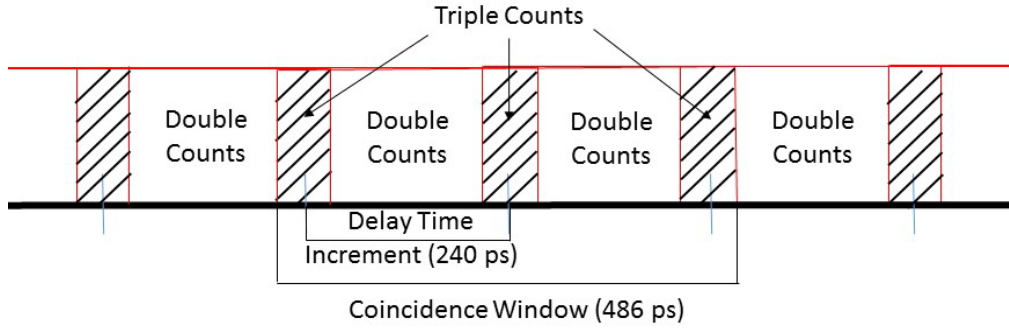


Figure 6. Explanation of coincidence count scaling by a factor of 240/486. The blue tick marks indicate delay times of coincidence measurements while the red boxes indicate coincidence windows for these measurements (not to scale). Double or triple counts correspond to double or triple overlap of the red boxes.

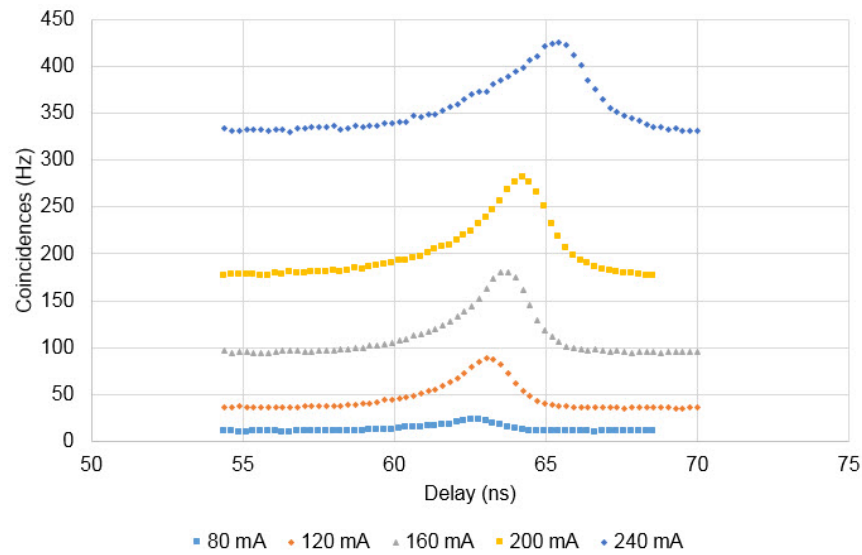


Figure 7. Coincidences detected at a series of pump currents.

The coincidence counts for several values of pump current are shown in Figure 7. The peak in detected coincidences corresponds to the delay at which the signals from two entangled photons are arriving at the same time. The nonzero level of coincidences far from the peak indicates the measurement of accidental coincidences. The summation of a coincidence curve, with the floor of accidental coincidences subtracted away, yields the total number of true coincidences detected. The nonzero width of the coincidence peak is due to jitter in the detectors and the delay generators along with the finite width of the coincidence window. True and accidental coincidences are shown in Figure 8 as a function of laser current.

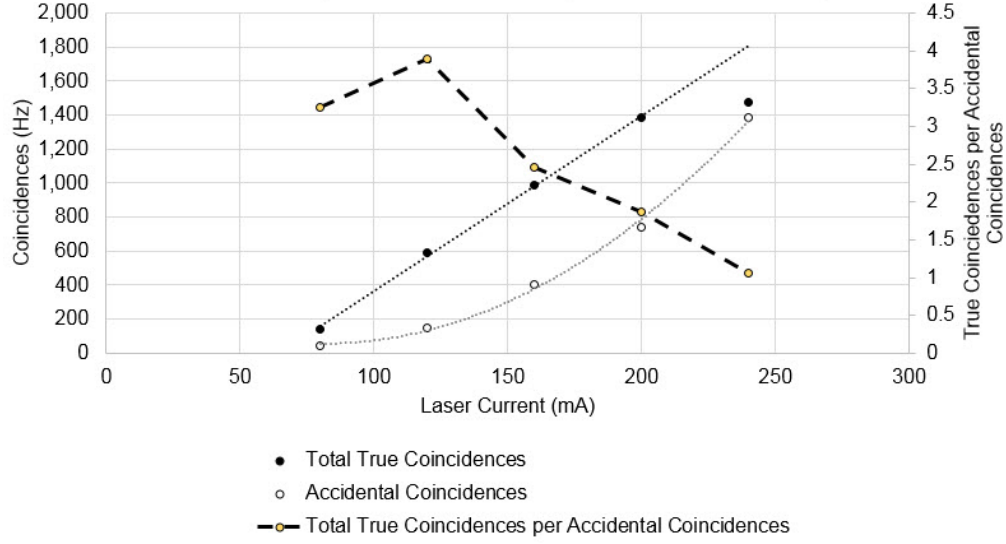


Figure 8. Total true coincidences versus laser current; the displayed fit includes the four points in the linear region of operation. Here accidental coincidences are integrated over a 1 ns delay time compared to the true coincidences which were integrated over the entire coincidence window. The yellow circles connected by the bold long-dashed lines indicate the ratio of total true coincidences to accidental coincidences.

From Figure 8, we see that accidental coincidences increase quadratically while true coincidences generally increase linearly. We also observe that for currents above 200 mA, the true coincidences detected stop increasing with increasing laser current. When combined with the increasing accidental coincidences this phenomenon leads to increasingly poor results in this regime, which is why we did not conduct studies at currents higher than 240 mA. The fact that the ratio between true and accidental coincidences is maximized at 120 mA is also significant; this will be further discussed in Section 5.2.

Accidental coincidences are directly correlated to counts at each detector as well as the coincidence window in which they are detected. Accidental coincidence rates are predicted by the following formula:

$$D_{AC} = D_{800} * D_{1600} * \tau, \quad (3)$$

where D_{AC} is detected accidental coincidence rates, D_x is detected coincidence rates at wavelength x (in nm), and τ is the width of the integration in nanoseconds. Figure 9 shows that this calculation is in good agreement with the experimental values.

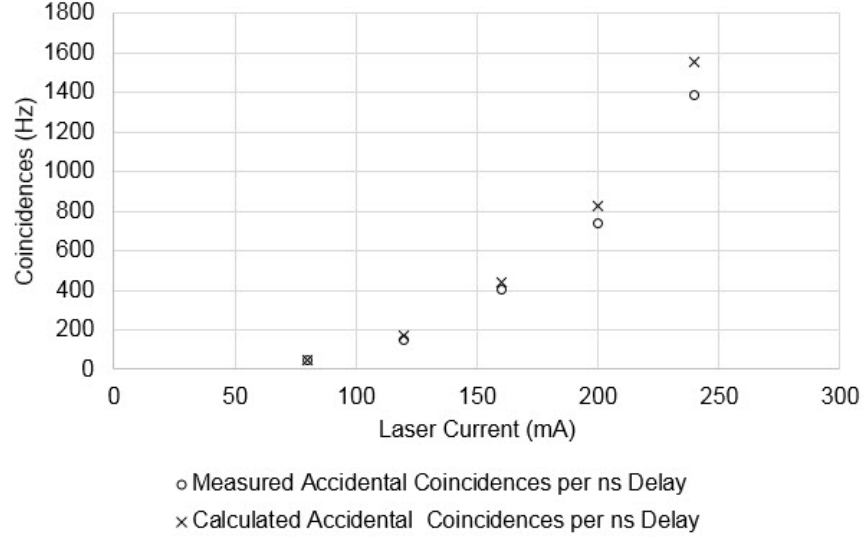


Figure 9: Measured and predicted accidental coincidences integrated over 1.0 ns delay time ($\tau = 1$ ns) as a function of laser current.

3.4 Photon-Pair Generation Calculation

Figure 10 shows the average detection rate at each wavelength as a function of current. The following procedure describes how we use these data, combined with the total true coincidences shown in Figure 8, to calculate total entangled pairs generated at the source.

The number of photons detected (after dark counts are subtracted) at each wavelength is described by the following equations:

$$D_{800} = E_{800} * G_{800} \quad (4)$$

and

$$D_{1600} = E_{1600} * G_{1600} \quad (5)$$

where E_x is the total path efficiency of wavelength x and G_x is the photon generation rate at the source of wavelength x . However, because the source only generates 800- and 1600-nm photons in pairs we have:

$$G = G_{800} = G_{1600}. \quad (6)$$

If the path efficiencies are independent, then

$$D_{TC} = E_{800} * E_{1600} * G \quad (7)$$

where D_{TC} is the detected true coincidences per second. Combining equations 4-7 we find that

$$G = \frac{D_{800} * D_{1600}}{D_{TC}}. \quad (8)$$

Equation 8 is used to calculate the data displayed in Figure 11 from our observations.

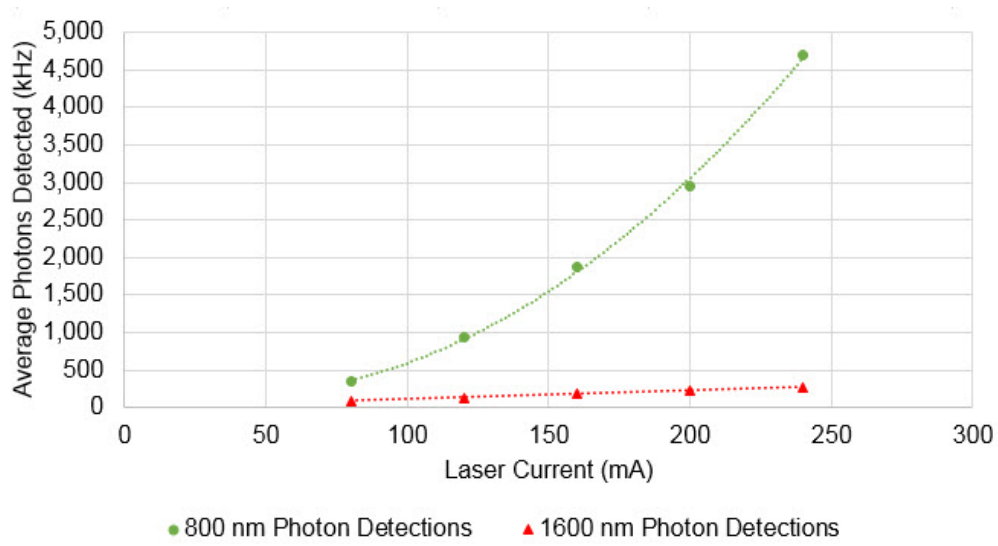


Figure 10. Photon detection rates as a function of laser current. The photons detected are averaged over approximately 10,000 collected data points and previously measured dark counts are subtracted out.

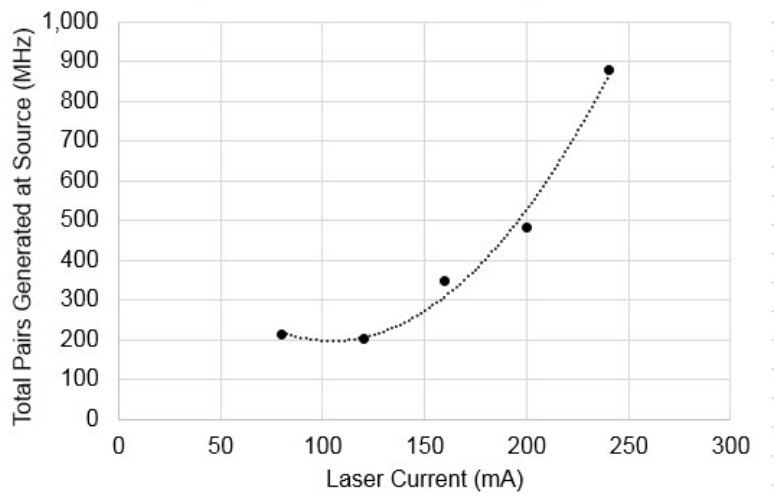


Figure 11. Total pair generation rate as a function of laser current. The pair generation rate is calculated based upon the individual photon detection rates and the total true coincidence rates.

4. FREE-SPACE QUANTUM KEY DISTRIBUTION DEMONSTRATION

4.1 Experimental Design

After characterizing the PP KTP entangled photon source, we proceeded to demonstrate free-space QKD via the B92⁵ protocol. In B92, a key is distributed between Alice and Bob in the manner described in Table 1. In this protocol, Alice prepares a random string of 0's and 1's which are encoded in the polarization states $|0^0\rangle$ and $|1-45^0\rangle$ respectively. The polarization-encoded photons are then sent to Bob. Bob measures the photons in the $|45^0\rangle$ (corresponding to the bit

value 0) and the $|90^\circ\rangle$ (corresponding to the bit value 1) bases which are randomly chosen. Consider the case corresponding to the first row of Table 1. Alice sends a $|0^\circ\rangle$ polarized photon and Bob measures in the $|45^\circ\rangle$ basis. Bob has a 50% chance of detecting this photon and if he does he announces through a public channel that he has a detection and both Alice and Bob add a ‘0’ to their secure bit stream. If he does not detect it, nothing is added to the key. In the case of the second row, Alice sends a $|0^\circ\rangle$ polarized photon and since Bob measures in the $|90^\circ\rangle$ basis, he does not detect it. Likewise in the third row, he does not detect the $|45^\circ\rangle$ polarized photon with his $|45^\circ\rangle$ basis. In the case of the fourth row, Alice sends an $|45^\circ\rangle$ polarized photon and Bob has a 50% chance of detecting it with his $|90^\circ\rangle$ basis. If he detects it, he publicly announces a detection, and both he and Alice add a ‘1’ to their secure bit stream. If an eavesdropper (Eve) between Alice and Bob detects a photon in a basis other than that in which it was sent, the polarization will change and she will reveal her presence. Although not as efficient as the original QKD protocol, BB84⁶, it is an attractive alternative because Alice must generate only two polarization states instead of four and because classical transmission only has to go in one direction (from Bob to Alice).

Table 1. B92 protocol. 75% of Bob’s measured photons—denoted by “-” —are indeterminate and therefore do not contribute to the final key.

Alice’s Bit/Basis	Bob’s Bit/Basis	Bob’s Measurement	Bob’s Bit
0 / $ 0^\circ\rangle$	0 / $ 45^\circ\rangle$	Yes/No	0 / -
0 / $ 0^\circ\rangle$	1 / $ 90^\circ\rangle$	No	-
1 / $ 45^\circ\rangle$	0 / $ 45^\circ\rangle$	No	-
1 / $ 45^\circ\rangle$	1 / $ 90^\circ\rangle$	Yes/No	1 / -

Implementing B92 only requires single photons rather than entangled photons. We chose to use the 800-nm photons because of our superior detection efficiency at that wavelength. The photons are generated, sorted, and collimated as described in Section 3.1. After collimation, the photons pass through a polarizing filter before entering a FastPulse Technology, Inc. Pockels cell driven by a FastPulse model GA-21R wide-band amplifier with a rated frequency response of ≥ 4.5 MHz. The amplifier is controlled with a Tektronix AWG5002B Arbitrary Waveform Generator (AWG), which outputs a random sequence of one of two voltages corresponding to a 0° or -45° polarization rotation from the Pockels cell (Alice’s bit/basis). The random sequence is produced by LabVIEW’s pseudorandom number generator. After leaving Alice’s Pockels cell, the photons travel over 0.4 meters of free space before entering Bob’s Pockels cell. Bob’s Pockels cell is driven via another wide-band amplifier with a different random sequence of one of two voltages from a different output of the same AWG corresponding to a 45° or 90° polarization rotation (Bob’s basis). The photons then pass through or are reflected by a Thorlabs PBS252 polarizing beam-splitter before detection at one of two PerkinElmer SPCM-AQR-13 silicon avalanche photodiode modules (Bob’s measurement). These detections go to the ID800 time tagger and are later compared to Bob’s basis and translated into a key via the method shown in Table 1. The time tags are also compared with Alice’s bit/basis for her own key generation. The two keys are then compared to determine bit error rate.

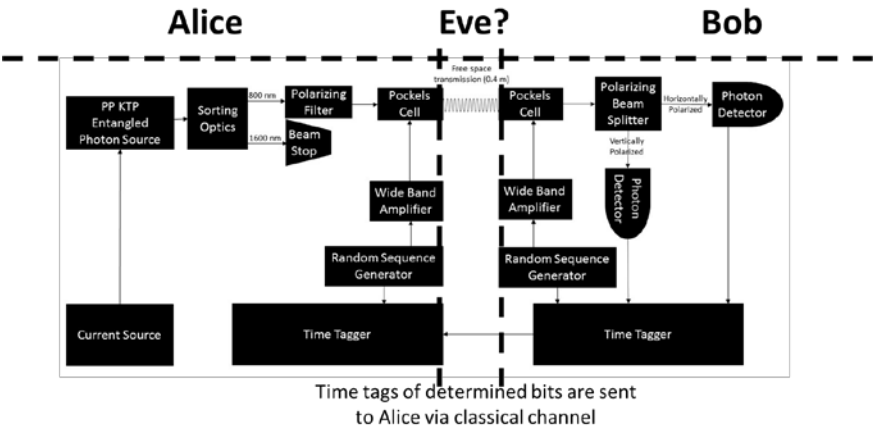


Figure 12. B92 experimental design.

4.2 B92 Results

We performed B92 across a range of parameters, measuring bit rate and bit error rate. We were also cognizant of the ratio of single photon-to-multiple photon (as measured coming out of Alice's Pockels cell). We use the factor μ to denote this security metric:

$$\mu = \frac{P_1}{P_{\geq 1}}. \quad (9)$$

where P_1 is the probability of registering a single count and $P_{\geq 1}$ is the probability of registering more than a single count. This ratio is calculated assuming the time distribution of the spontaneous parametric down-conversion (SPDC) emissions is a Poisson distribution. The ratio can be increased by increasing the frequency of Pockels cell modulation or by decreasing the pump laser current.

We first swept pump laser current from 80 mA to 240 mA while keeping the Pockels cell modulation frequency constant at 4 MHz. The results are shown in Figure 13. Basic filtering in which photons were discarded if they fell within the portion of the modulation period corresponding to the rise- or fall-time of the amplifier, was applied to all of the following results. Bit error rates for the data in Figure 13 range from 9.7% to 13.4%.

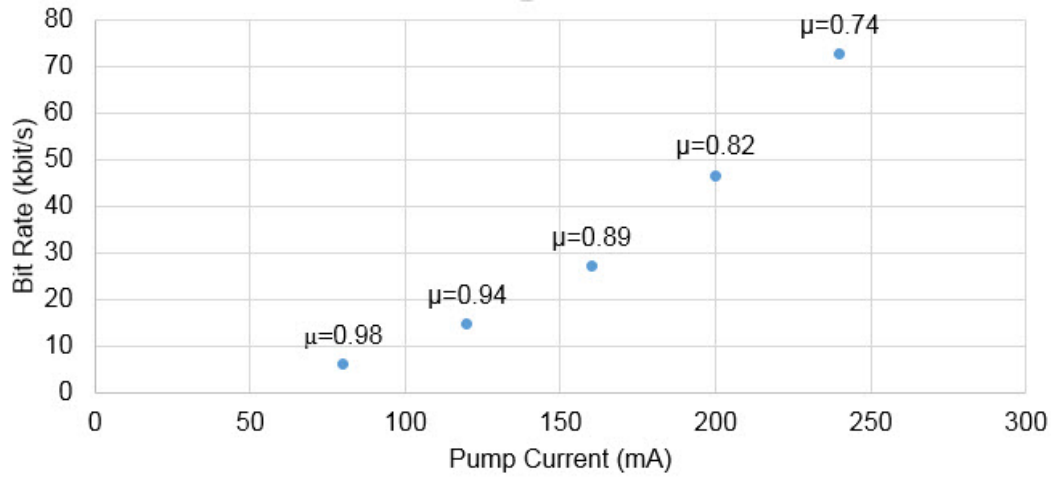


Figure 13. Bit rate versus laser pump current at a Pockels cell modulation frequency of 4 MHz. In order to take advantage of the high bit rates measured at higher currents, one must modulate at higher frequencies to keep μ at 0.9 or higher.

Next, we varied Pockels cell modulation frequency while adjusting pump current to keep μ constant at 0.9 (Figure 14). There is steady improvement in the bit rate as the frequency increases up to 4 MHz, where the bit rate is 31.6 kbit/s. However, we find significant losses at frequencies over 4 MHz (and the corresponding detection rates associated with maintaining $\mu=0.9$) due to the data transfer rate limitation via the USB 2.0 interface between the computer and the time tagger. We find this data loss to be the primary limiting factor of the setup, although we are also approaching the maximum rated modulation frequency of the wide-band amplifiers.

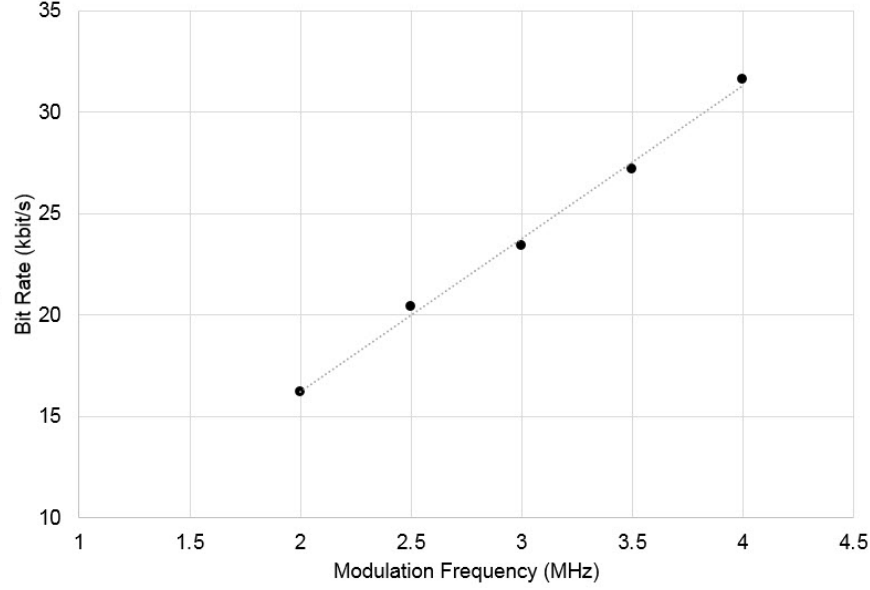


Figure 14. Bit rate versus modulation frequency as μ is held constant at 0.9. The 4 MHz data point has a bit rate of 31.6 kbits/s and a bit error rate of 10.5%.

5. DISCUSSION

5.1 Comparison of B92 to BB84

Our implementation of B92 is not fully secure for a number of reasons. One is that the bits and bases chosen by Alice and Bob are generated by pseudorandom rather than a truly random source. Another security compromise is that even with $\mu = 0.9$, we have not accounted for the other 0.1. This could be ameliorated by privacy amplification⁷, which would decrease the true bit rate, or by using decoy states⁸. Most notably, B92 as we have implemented it, is vulnerable to the intercept-resend attack in which Eve randomly measures polarization states just as Bob would, killing the 75% of photons that she does not positively identify, and sending the remaining 25% in the determined polarization state on to Bob. Bennett⁵ proposed a solution, but we do not have a means of doing so in our set-up. BB84 is not vulnerable to such an attack because Eve would not know which bits she had correctly identified until after transmission, when Alice and Bob compare bases. The only factor limiting us from running BB84 with our setup is our amplifier, which is not capable of applying the necessary 135° range of polarization rotation. Switching from B92 to BB84 would also improve our bit rate and bit error rate. BB84 converts 50% rather than 25% of detected photons into key material, meaning that bit rates would be approximately doubled. Bit error rates would also be about halved.

5.2 Noise-Resistant Coincident Photon Protocols

While we have successfully implemented B92 using only one of the entangled pairs of photons, in the future we would like to use coincident detections to implement more noise-resistant protocols such as quantum illumination⁹. Such a protocol would require the construction of a plot like that of Figure 7. Then, the receiver has to determine which photons to consider. For example, we might consider a 0.96 ns window around the peak of the 120 mA coincidence peak, as illustrated in Figure 15.

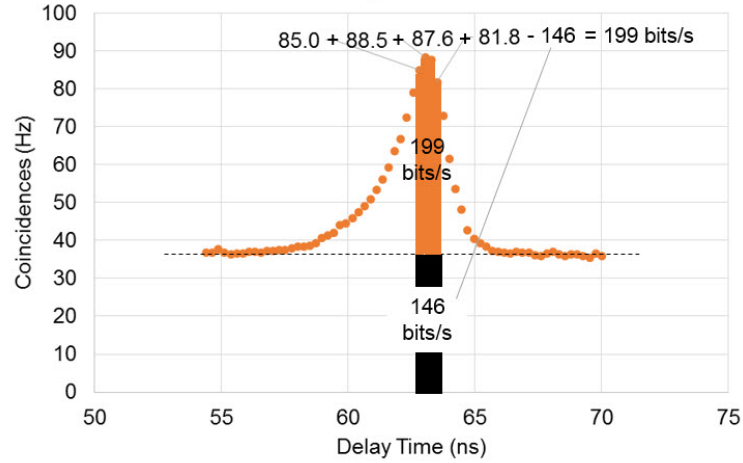


Figure 15. A 0.96 ns delay window around the peak of the 120 mA coincidence curve. The orange area indicates true coincidences, the dashed line indicates the noise floor, and the black rectangle indicates accidental coincidences.

The two important factors to consider in such an experiment are bit rate and signal-to-noise ratio (SNR). In practice, to calculate the bit rate for a given window, we simply perform a Riemann sum of data points. For the example above, to calculate the bit rate for a 0.96 ns window, we add the 4 largest data points on the curve and subtract the accidental coincidence floor (i.e., we calculate the orange area). This yields a bit rate of 199 Hz and an SNR of $199/146 = 1.35$. Notice that increasing the window width will increase the bit rate but decrease the SNR. The question then arises: what pump current and bin window provides the optimal balance between bit rate and SNR?

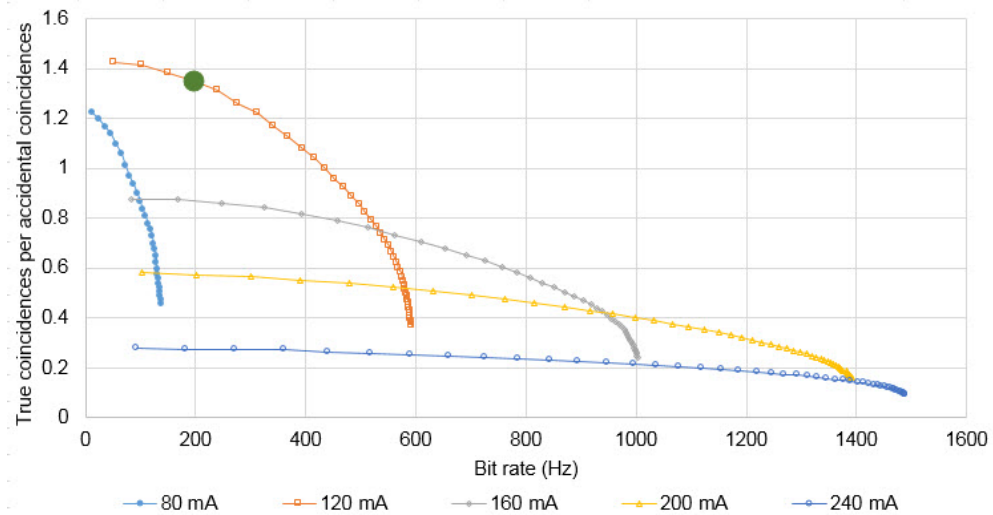


Figure 16. SNR as a function of bit rate for each pump current studied. Each point on the graph represents an additional 240 ns of window width. The large green dot indicates the data point represented by Figure 15.

From Figure 16, it can be seen that while the optimal laser current depends upon what bit rate we would like to obtain, 120 mA achieves the best bit rates if a SNR of 0.8 or above is desired. This current is optimal in our system for two reasons. Firstly, in Figure 8, we see that the ratio of total true coincidences to accidental coincidences is maximized at 120 mA. Secondly, the width of the coincidence peak increases significantly for currents above 160 mA (Figure 17),

leading to greatly decreased SNR at these currents. In the future, we plan to remove the delay generators from the set-up in order to decrease the jitter in our system, narrow the coincidence peaks, and increase SNR for all pump currents.

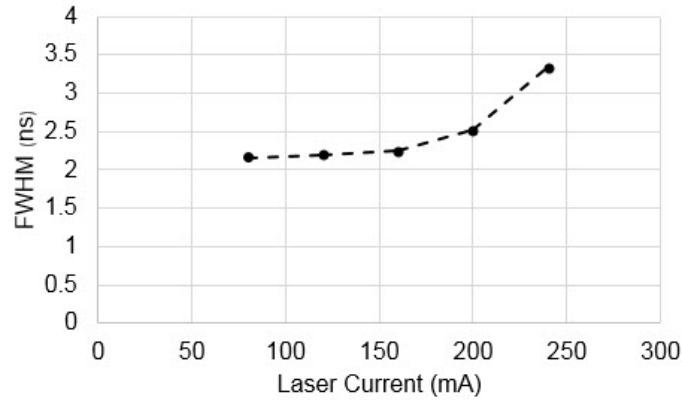


Figure 17: FWHM of the coincidence curves (Figure 7) as a function of laser current.

It can be seen that while we are calculating pair generation rates of 200-880 MHz (Figure 11), we are recording total true coincidence rates of just 490-1450 Hz, (Figure 9). The losses are a consequence of the efficiencies of each signal chain, as described in Equation 7. Equations 4, 5, and 6 allows us to calculate individual path efficiencies at each laser current. These results are shown in Figure 18.

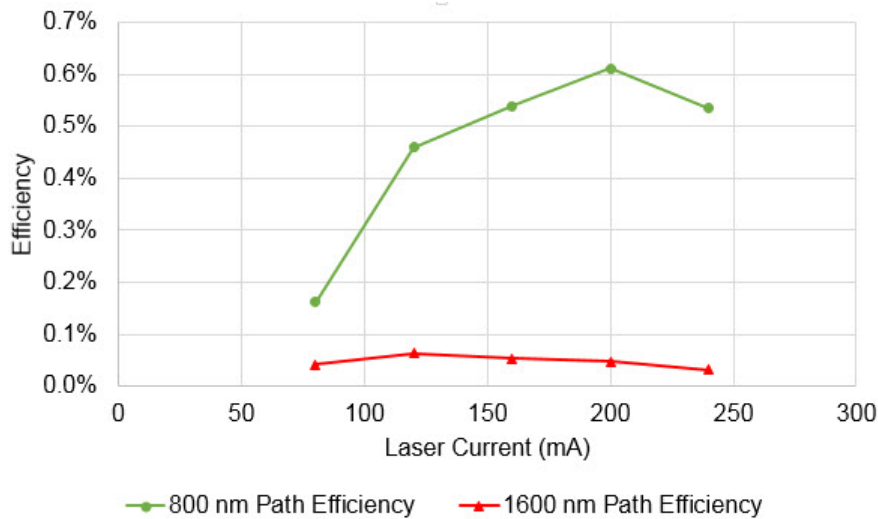


Figure 18. Path efficiencies (photons detected divided by calculated pairs generated) as a function of laser current.

The reason for the significantly lower path efficiencies at 80 mA may be because this is close to the threshold current and the generation process is nonlinear. The decreasing 1600-nm path efficiency with laser current, as well as the linear (rather than quadratic) increase of the 1600-nm photon detections (Figure 10), are thought to be due to the 1 μ s dead time of the 1600-nm InGaAs detector, which causes it to be dead for 14-33% of the time as the current is increased from 80-240 mA. The discrepancy between the 800-nm path and the 1600-nm path efficiencies seen in Figure 18 is primarily due to the comparative detection rates of the two sources: the 800-nm Si detector is 62% efficient⁴, while the 1600-nm InGaAs detector is only 3.5% efficient¹⁰. A summary of path efficiency losses at 120 mA is shown in Table 2.

Table 2. Path efficiency breakdown at 120 mA. Shaded values are assumed constant regardless of laser current. “Total Uncharacterized Effects” may be due to losses in the waveguide after down-conversion, imperfect fiber couplings, and, in the case of the 800-nm photons, free space attenuation.

Signal Chains	Filters in Sorting Optics	Detection Efficiency	Dead Time Effect	Total Characterized Effects	Total Uncharacterized Effects	Path Efficiency
800 nm	0.484	0.620	0.954	.286	.016	0.460%
1600 nm	0.689	0.035	0.817	.020	.032	0.064%

A significant improvement to our system can be achieved by replacing the InGaAs detector with a higher efficiency 1600-nm photon detector. Superconducting nanowire detectors exist¹¹ that have detector efficiencies greater than 60% at 1600 nm along with decreased dead time, dark counts, and jitter. Preliminary estimates indicate that bit rates of over 10 kHz with an SNR of over 1.5 are possible with a superconducting nanowire detector placed into our current setup; we are in the process of gaining access to such a detector.

6. CONCLUSIONS

Measurements indicate that a periodically-poled potassium titanyl phosphate (PP KTP) waveguide source developed by AdvR, Inc. generates polarization-entangled photon pairs at a rate of 880 MHz when pumped with a current of 240 mA and could likely output even higher rates at higher currents. This generation rate is orders of magnitude higher than those reported from conventional beta barium borate (BBO) crystal spontaneous parametric down-conversion (SPDC) entangled photon sources^{12, 13}. Such high generation rates, especially with entangled pairs that can potentially be used to cancel noise, are critical for practical QKD.

A preliminary demonstration of secure free-space communication with the PP KTP source with a bit rate of 31.6 kHz and a bit error rate of 10.5% is also encouraging. This bit rate is about an order of magnitude short of some of the best results in the literature,^{8, 14} but we expect to be able to significantly improve these results since the bit rate is limited not by our photon source but rather by the switching speed of the amplifiers and the data transfer rate from the time tagger. With equipment improvements we project that we could generate secure keys at a rate of 1 MHz and a bit error rate of 6.3% with BB84 QKD. This is comparable to rates with state-of-the-art QKD systems, with the added benefit of generating entangled photons which have the potential to be used for noise cancellation.

REFERENCES

- [1] Slattery, O., Ma, L., and Tang, X., "Optimization of photon pair generation in dual-element PPKTP waveguide," *Proc. SPIE* 7465 (2009).
- [2] Baldi, P., Aschieri, P., Nouh, S., De Micheli, M., Ostrowsky, D. B., Delacourt, D., and Papuchon, M., "Modeling and experimental observation of parametric fluorescence in periodically poled lithium niobate waveguides," *IEEE J. Quant. Elec.* 31(6), 997-1008 (1995).
- [3] Bonfrate, G., Pruneri, V., Kazansky, P. G., Tapster, P., and Rarity, J. G., "Parametric fluorescence in periodically poled silica fibers," *Appl. Phys. Lett.* 75(16), 2356-2358 (1999).
- [4] PerkinElmer, "SPCM-AQR single photon counting module," (2001).
< http://sites.fas.harvard.edu/~phys191r/Bench_Notes/D4/SPCMAQR.pdf >.
- [5] Bennett, C. H., "Quantum cryptography using any two orthogonal states," *Physical Review Letters*, 68(21), 3121-3124 (1992).
- [6] Bennett, C. H. and Brassard, G., "Quantum cryptography: public key distribution and coin tossing," *Proc. Of IEEE International Conference on Computer Systems and Signal Processing*, Bangalore, India, 175-179 (1984).
- [7] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J., "Experimental quantum cryptography," *Journal of Cryptography*, 5(1), 3-28 (1992).
- [8] Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W., and Shields, A. J., "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Opt. Express* 16(23), 18790-18797 (2008).
- [9] Shapiro, J. H., "Defeating passive eavesdropping with quantum illumination," *Phys. Rev. A* 80, 022320 (2009).
- [10] ID Quantique, "Infrared Single-Photon Counting System," (2014).
<<http://marketing.idquantique.com/acton/attachment/11868/f-007a/1/-/-/-/ID210%20Datasheet.pdf>>.
- [11] Hadfield, R. H., "Single-photon detectors for optical quantum information applications," *Nature Photonics*, 3(12) 696-705 (2009).
- [12] Takeuchi, S., "Recent progress in single-photon and entangled-photon generation and applications," *Japanese Journal of Applied Physics*, 53(3) 030101 (2014).
- [13] Lekki, J. D., Nguyen, Q.-V., Nguyen, B. V., and Hizlan, M., "Quantum optical communication for micro robotic explorers," *Proc. AIAA Infotech@ Aerospace Conf.* (2005).
- [14] Sasaki, M. et al., "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express* 19(11), 10387-10409 (2011).